CLAIMS

What is claimed is:

1. A method for exchanging a secure cryptographic key for a quantum cryptography apparatus employing non-ideal elementary quantum systems, wherein

- the apparatus comprises an emitter and a receiver, being connected by a quantum channel and a conventional communication channel,
- the emitter encodes each bit at random onto a pair of non-orthogonal states belonging to at least two suitable sets,
- there is no a single quantum operation reducing the overlap of the quantum states of all sets simultaneously,
- the emitter sends the encoded bit along the quantum channel to the receiver,
- the receiver randomly chooses the analysis measurement within said suitable sets,
- the emitter sends the set information along the conventional communication channel,
- the receiver discards all received encoded bits for which he has chosen a different analysis measurement incompatible with the set they belonged to and sends an appropriate information to the emitter along the conventional communication channel.

2. The method according to claim 1, wherein in the step of the emitter sending an encoded bit along the quantum channel to the receiver weak coherent states are exchanged between the emitter and the receiver.

3. The method according to claim 2, wherein the weak coherent states are laser pulses with an average photon number per pulse of less than 0,5 photons, preferably less than 0,1 photons.

4. The method according to claim 1,

- wherein the emitter is using two sets A $=\{|0_a\rangle,|1_a\rangle\}$ and B $=\{|0_b\rangle,|1_b\rangle\}$, chosen such that $|\langle 0_a|1_a\rangle|=\eta_a\neq 0$, $|\langle 0_b|1_b\rangle|=\eta_b\neq 0$, and wherein there is no single quantum operation reducing the overlap of the quantum states of all sets simultaneously, and

- the receiver randomly chooses the analysis measurement between

$$F_A = \frac{1}{\sqrt{1+\eta}}\left(\left|+x\right\rangle\left\langle 1_a^\perp\right| + \left|-x\right\rangle\left\langle 0_a^\perp\right|\right) \text{ and } F_B = \frac{1}{\sqrt{1+\eta}}\left(\left|+x\right\rangle\left\langle 1_b^\perp\right| + \left|-x\right\rangle\left\langle 0_b^\perp\right|\right)$$

followed by a Von Neumann measurement distinguishing between $\left|+x\right\rangle and \left|-x\right\rangle$.

5. The method according to one of claims 1 to 4, wherein after a number of encoded bits has been transmitted, a protocol step is performed, within which emitter and receiver agree on a body of cryptographic key information which is shared between emitter and receiver, but secret from all other units who may be monitoring the quantum channel and the public channel, or else conclude that the encoded bits can not be safely used as cryptographic key information.

6. A method for exchanging a secure cryptographic key for a quantum cryptography system employing non-ideal elementary quantum states, where the key values are encoded on at least two sets of non-orthogonal quantum states characterized by the fact that it is not possible to find a single quantum operation, whether probabilistic or not, that reduces the overlap of the states of all sets simultaneously.

7. A quantum cryptography system employing non-ideal elementary quantum states to exchange secure cryptographic key information and comprising

- a source of non-ideal elementary quantum states,
- an emitter and a receiver, being connected by a quantum channel and a conventional communication channel,
- the emitter comprising or connected to a random number generator allowing to prepare random non-orthogonal quantum states belonging to at least two suitable sets, wherein there is no single quantum operation reducing the overlap of the quantum states of all sets simultaneously,
- the receiver comprising or connected to a random number generator allowing to choose an analysis measurement for said quantum states,
- the emitter being able to send the encoded bit along the quantum channel to the receiver and being able to send the set information along the conventional communication channel,

- the receiver being able to discard all received encoded bits for which he has chosen a different analysis measurement and to send an appropriate information to the emitter along the conventional communication channel.

8. The quantum cryptography system according to claim 7, wherein said source is a laser source and the emitter comprises a preparation device sending laser pulses with an average photon number per pulse of less than 0,5 photons, preferably less than 0,1 photons.

9. The quantum cryptography system according to claim 7, wherein emitter and receiver both comprise processing units being able to perform, after a number of encoded bits had been transmitted, a protocol step, within which emitter and receiver agree on a body of cryptographic key information which is shared between emitter and receiver, but secret from all other units who may be monitoring the quantum channel and the public channel, or else conclude that the encoded bits can not be safely used as cryptographic key information.

10. The method according to claim 1, wherein for each bit, the emitter is randomly using one of the four states $|\pm x\rangle$ or $|\pm y\rangle$ with the convention that $|\pm x\rangle$ code for 0 and $|\pm y\rangle$ code for 1, and sends it along the quantum channel to the receiver, the receiver randomly measures σ_x or σ_y, the emitter announces one of the four pairs of non-orthogonal states $A_{\omega,\omega'} = \{|\omega_x\rangle, |\omega'_y\rangle\}$ with w,w'$\in \{+,-\}$ and such that one of the states is the one which he has sent by sending an appropriate message along the conventional communication channel, the receiver discards all received encoded bits for which the measurement result he has obtained is possible for both states disclosed by the emitter and sends an appropriate information to the emitter along the conventional communication channel, the receiver deduces the state actually sent by the emitter and adds the corresponding bit to the key.